

1

الهاكر الأخلاقي

المقدمة (Introduction)

By

Dr.Mohammed Sobhy Teba
Introduction
https://www.facebook.com/tibea2004

CONTENTS

INTRODUCTION TO ETHICAL HACKER

"إذاً، إذا كنت تعرف العدو وتعرف نفسك – فلا حاجة بك للخوف من نتائج مئة معركة. إذا عرفت نفسك لا العدو، فكل نصر تحرزه سيقابله هزيمة تلقاها. إذا كنت لا تعرف نفسك أو العدو – ستنهزم في كل معركة"
كتاب فن الحروب للعبقري والفيلسوف العسكري الصيني سون تزو

في عصرنا الحالي انقلبت الموازين، أصبح الصغار كبارا بعقولهم في عالم الهاكر أعمارهم تتراوح ما بين ال 16 سنة وال 20 سنة. في هذا السن تجد كثيرون محترفون في عالم الهاكرز، منهم الطيب ومنهم الخبيث، المخترقون أجناس. وقد تجد فيهم من يساعد الناس في استرجاع بياناتهم وبريدهم الالكتروني. ومنهم من يقوم بسرقة الناس مدعيا انه شخص طيب وهو في الأصل متلصص يريد أن يخترق عبثا، كثرت عمليات الاختراقات في العالم العربي. ولاحظنا الاختراقات الكثيرة على المواقع العربية وبأيدي عربية للأسف. أصبح الهاكر وسيلة للتهديد ووسيلة للانتقام وأصبح وسيلة للاستفادة من الأشخاص إما من اجل المال أو شيء يريده ولم يجده إلا عند شخص ما، هذه الثلاثة من اغلب ما يحدث بين ما يسمون بالهاكر. لذلك فمن المهم جدا أن نضع في اعتباراتنا أن الهاكر يعمل على كسر الشبكة الخاصة بك والأنظمة التي تحتويها من اجل العديد من الأسباب والأهداف، لذلك فانه من المهم فهم كيفية اختراق المهاجمين الهاكرز للأنظمة واستغلال الثغرات وأيضا معرفة الهدف من هذا الهجوم.
من الواجب على كل من مديري الأنظمة (**ADMIN**) ومحترفي الأمن في الشبكات (**network security prof.**) القيام بحماية البنية التحتية لأنظمتهم (**infrastructure**) من الثغرات وذلك بمعرفة العدو (الهاكرز) وما الذي يسعى إليه من استخدام أنظمتك (استغلالها في الأنشطة الغير قانونيه والضارة) وهذا هو المغزى من المقولة السابقة من كتاب فن الحرب.

ما هو الهاكرز؟

أُطلقت هذه الكلمة أول ما أطلقت في الستينيات لتشير إلى المبرمجين المهرة القادرين على التعامل مع الكمبيوتر ومشاكله بخبرة ودراية حيث أنهم كانوا يقدمون حلولا لمشاكل البرمجة بشكل تطوعي في الغالب.
بالطبع لم يكن الويندوز أو ما يعرف بالـ **Graphical User Interface** أو **GUI** قد ظهرت في ذلك الوقت ولكن البرمجة بلغة البيسيك واللوغو والفور توران في ذلك الزمن كانت جديرة بالاهتمام. ومن هذا المبدأ غدا العارفين بتلك اللغات والمقدمين العون للشركات والمؤسسات والبنوك يعرفون بالهاكرز وتعني الملمين بالبرمجة ومقدمي خدماتهم للآخرين في زمن كان عددهم لا يتجاوز بضع ألوف على مستوى العالم أجمع. لذلك فإن هذا الوصف له مدلولات إيجابية ولا يجب خلطه خطأ مع الفئة الأخرى الذين يسطون عنوه على البرامج ويكسرون رموزها بسبب امتلاكهم لمهارات فئة الهاكرز الشرفاء. ونظرا لما سببته الفئة الأخيرة من مشاكل وخسائر لا حصر لها فقد أطلق عليهم إسماً مرادفا للهاكرز ولكنه يتداول خطأ اليوم وهو (**الكراكرز Crackers**) كان الهاكرز في تلك الحقبة من الزمن يعتبرون عباقرة في البرمجة فالهاكر هو المبرمج الذي يقوم بتصميم أسرع البرامج والخالي في ذات الوقت من المشاكل والعيوب التي تعيق البرنامج عن القيام بدورة المطلوب منه. ولأنهم كذلك فقد ظهر منهم إسمان نجحا في تصميم وإرساء قواعد أحد البرامج المستخدمة اليوم وهما دينيس ريتشي وكين تومسون اللذان نجحا في أواخر الستينيات في إخراج برنامج اليونيكس الشهير إلى حيز الوجود. لذلك فمن الأفضل عدم إطلاق لقب الهاكر على الأفراد الذين يدخلون عنوه إلى الأنظمة بقصد التطفل أو التخريب بل علينا إطلاق لقب الكراكرز عليهم وهي كلمة مأخوذة من الفعل **Crack** بالإنجليزية وتعني الكسر أو التحطيم وهي الصفة التي يتميزون بها.

ما هو الهاكر الأخلاقي ETHICAL HACKING؟

هو عملية فحص واختبار الشبكة الخصه بك من اجل إيجاد الثغرات ونقاط الضعف والتي من الممكن أن يستخدمها الهاكرز. الشخص الذي يقوم بهذه العملية هو الهاكر الأبيض (**white hacker**) الذي يعمل على الهجوم على أنظمة التشغيل بقصد اكتشاف الثغرات بها بدون الحاق أي ضرر. وهذا من الطبيعي يؤدى إلى زيادة معدلات الأمن لدى النظام الخاص بك. أو بمعنى أخر هو أنسان له مهارات تعطيه إمكانية الفهم والبحث عن نقاط الضعف في أنظمة التشغيل المختلفة، وهذا الشخص يعتبر نفسه هاكرز حيث يستخدم نفس معرفته ونفس أدواته ولكن بدون أن يحدث أي ضرر.

ما الفرق بين الهاكرز الأخلاقي والهاكرز العشوائي؟

- **الهاكرز الأخلاقي (ethical hacker):** هو خريج هذه الشهادة او ما يعادلها حيث يكتسب قوته من خلال خبرة أفضل هاكرز في العالم ويستخدمها في تحسين الوضع الأمني لأنظمة الشبكات المختلفة.
- **الهاكرز العشوائي** هو الهاكر المدمر.

في هذا الفصل سوف نتحدث عن المواضيع التالية:



1.2 رؤية مبسطه عن امن المعلومات (INFORMATION SECURITY OVERVIEW)

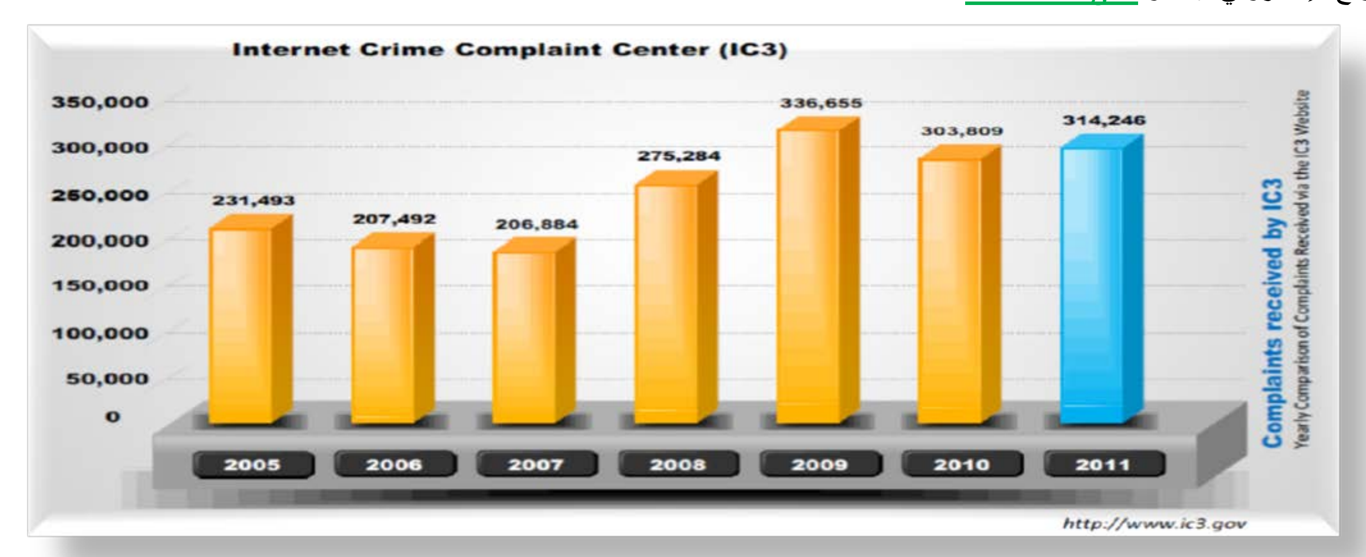
هذا المصطلح يشير إلى الطريقة المستخدمة لحماية أي نوع من المعلومات الحساسة او بمعنى أخر وضع حائط أمن حول المعلومات المهمة وذلك لحمايتها من قبل الاتي:

1. **Unauthorized access** الولوج/الوصول الغير مصرح به.
2. **Disclosure** الكشف عن هذه المعلومات.
3. **Alteration** التعديل على هذه المعلومات.
4. **Destruction** تدمير هذه المعلومات.

المعلومات تعتبر من المصادر الهامة لذلك يجب أن تكون أمنه، وذلك لان وقوع هذه المعلومات في الأيدي الخطأ قد يسبب تهديدا كبيرا على البنية التي تخصها هذه المعلومات.

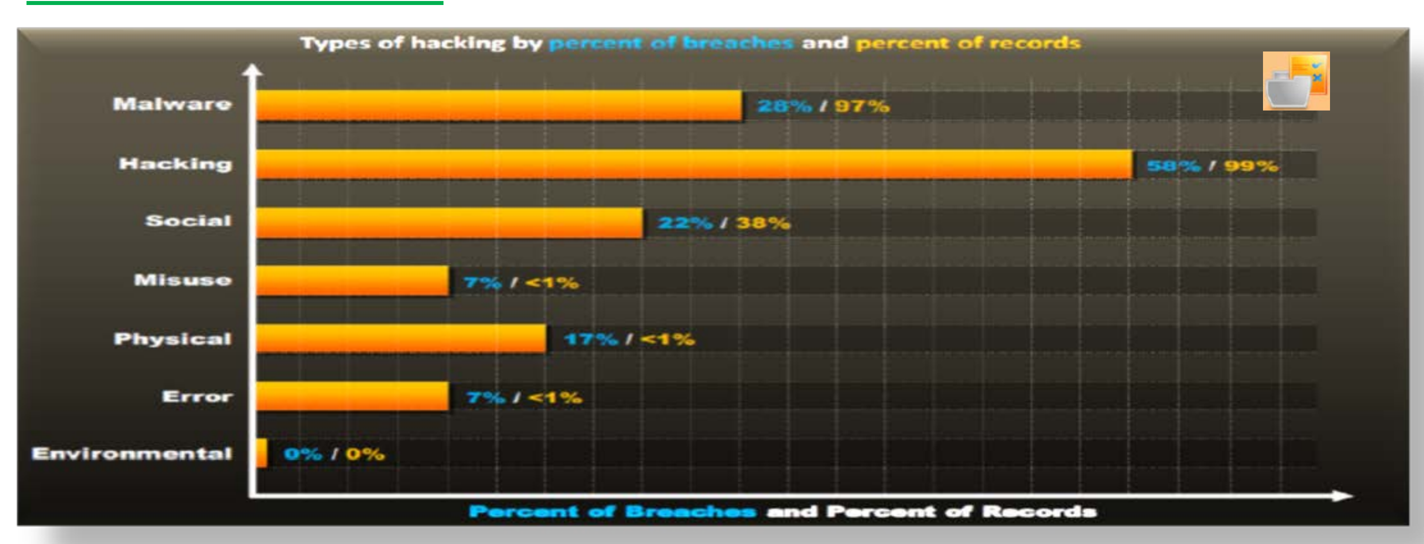
IC3

هو اختصار إلى **Internet Crime complaint center** وهي شركة تعمل على رصد الهجمات الإلكترونية ثم إعطاء تقرير عن هذا والموقع الإلكتروني لها هو **www.ic3.gov**



DATA BREACH INVESTIGATIONS REPORT (VERIZON BUSINESS)

شركه تعمل على رصد أنواع الهجمات وغيرها ثم تعطى تقرير عن هذا والموقع الإلكتروني الخاص بهم هو
www.verizonbusiness.com



بعض المصطلحات المهمة:

HACK VALUE

هو مفهوم بين الهاكرز على انه شيء مهم يستحق القيام به أو مثير للاهتمام أو بمعنى أخر هو قيمة العمل الذي سوف يقوم به.

EXPLOIT

هي طريقة اختراق نظام المعلومات من خلال نقاط الضعف الموجودة فيه وهذا المصطلح يستخدم في أي هجمه من أي نوع على الأنظمة والشبكات ويمكن أن يكون أيضا عباره عن تطبيقات أخرى أو أوامر (**commands**) والتي من الممكن أن تسبب سلوك غير متوقع لبرامج قانونيه أو أجهزه قانونية عن طريق اخذ ميزات نقاط الضعف التي تحتويها.

VULNERABILITY

هو مصطلح يعبر عن نقاط الضعف/الثغرات، وقد تكون نقاط الضعف هذه إما نقاط ضعف في التصميم (**design code**) أو أخطاء (**error/bugs**) والتي قد تسبب سلوك غير متوقع أو غير مرغوب فيه في نظام الأمن. وهو يعتبر المصدر الذي يهتم به الهاكر لكي يعمل عليه.

TARGET OF EVALUATION

هو نظام المعلومات أو الشبكات (**IT system**) أو برنامج أو محتوى يستخدم للوصول إلى درجه معينه من الأمن. وهذا النوع يساعد في فهم وظائف وتقنيات ونقاط الضعف في الأنظمة والمنتجات.

ZERO-DAY ATTACK

هو عباره عن هجوم يستغل ثغره امنيه لم تكن معروفه مسبقا للمبرمجين في تطبيق كمبيوتر وهذا يعنى أن المبرمجين لديهم صفر يوم لمعالجة هذا الضعف.

DAISY CHAINING

تعنى أن الهاكر الذي استطاع الوصول إلى قاعدة المعلومات فانه يعمل على تكملة أهدافه عن طريق تغطية أثار ما فعله ويتم ذلك بتدمير ملفات السجل (**destroy log file**) وذلك لإخفاء الهوية الخاصة به.

بعض المصطلحات التعريفية الأخرى:

- **Attack:** هو عباره عن أي هجوم على نظام امن.
- **Security**: عملية حماية البيانات من السرقة والعبث.
- **Threat**: الفعل أو الحدث الذى يمكن أن يضر بالأمن ، التهديد هو انتهاك محتمل للأمن.

عناصر امن المعلومات (ELEMENT OF INFORMATION SECURITY)

هي الحالة التي يكون فيها عملية جعل المعلومات والبنية التحتية للأنظمة (**Infrastructure**) من الصعب سرقتها وتتكون من خمس مراحل

Assurance that the information is accessible only to those authorized to have access

Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users

Guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

Confidentiality → Integrity → Availability → Authenticity → Non-Repudiation





The trustworthiness of data or resources in terms of preventing improper and unauthorized changes

Authenticity refers to the characteristic of a communication, document or any data that ensures the quality of being genuine



- **Confidentiality (الخصوصية)**

هي الإجابة على السؤال (من له الحق في الأطلاح/الدخول على هذه المعلومات؟) أو بمعنى اصح هي صلاحيات الدخول.

- **Integrity**

شكل البيانات (منع أي تغير على البيانات).

- **Availability (الإتاحة)**

البيانات تكون متاحه لمن له الحق في الدخول عليها أو بمعنى أخر أن النظام المسئول عن نقل وتخزين ومعالجة البيانات يكون متاحا لمن له الحق في الدخول عليها.

- **Authenticity**

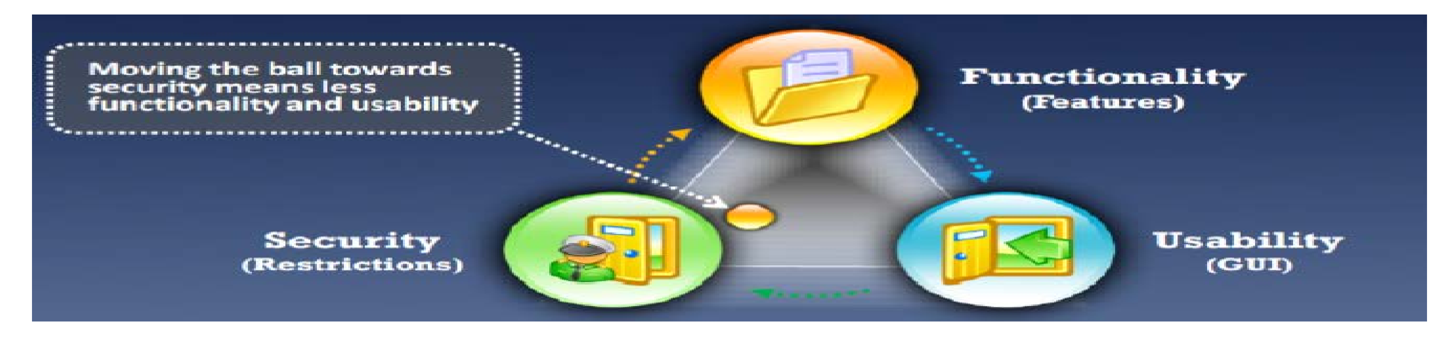
هذا يشير إلى سمة (الاتصالات، أو الوثيقة، أو أي بيانات) والتي تضمن نوعية كونها حقيقية أم لا (**genuine**) غير مقلده من الأصل.
والأدوار الرئيسية من عملية المصادقة **authentication** تشمل الاتي:

1. التأكيد من هوية المستخدم هل هو هذا المستخدم م المعرف لديه أم لا.
2. ضمان أن الرسالة القادمة منه اصليه ولم يتم التغير في محتواها أو ليست مزوره.
3. تستخدم كل من **biometric** و **smart cards** والشهادة الرقمية **digital certificate** في التأكد من مصداقيه البيانات أو الاتصال أو حتى المستندات.

- **Non-repudiation**

هذا يشير إلى القدرة على التأكد من أن طرفي العقد أو الاتصالات لا يستطيعا أن ينكرا صحة التوقيع على الوثيقة أو الرسالة المرسلة بينهم من الأمثلة على ذلك بروتكول **HTTPS** و **Kerberos**.

مستوى الأمان في أي من الأنظمة أو الشبكات الموجودة تتحد بقوة الثلاثة أشياء التالية:



حيث نلاحظ وجود دائرة صفراء والتي من الممكن أن تتحرك في أي زاوية من زاويا المثلث والتي تدل على معنى. حيث مكانها الحالي يدل انه مع زيادة الأمان (**security**) فانه سوف يقل الأداء (**Usability – Functionality**)

INFORMATION SECURITY THREATS AND ATTACK VECTOR 1.3

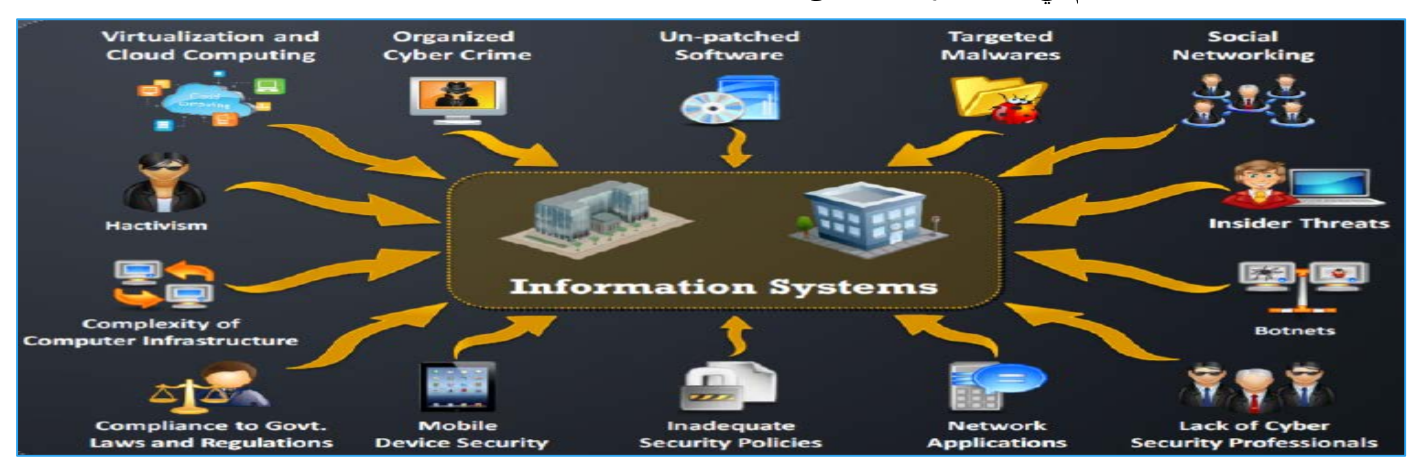
إن هذا الجزء يقدم لك الاتي:

1. **Attack Vector** من أين تأتى الهجمات؟
2. **Security Threat** التهديدات الأمنية المحتملة.
3. **Goal of attack** الهدف من وراء هذا الهجوم.

ATTACK VECTOR من أين يأتي هذا الهجوم؟

هذا يشير إلى المسار الذي يتخذه المهاجم للوصول إلى مركز المعلومات على أنظمة الشبكة لأداء بعض الأنشطة المختلفة.

Attack Vector: تمكن المهاجم من الاستفادة من الثغرات الموجودة في نظام المعلومات لحمل الهجوم الخاص به. المسارات المتاحة التي من الممكن أن يستخدمها المهاجم في عملية القرصنة كالاتى:



GOAL OF ATTACK الهدف من وراء هذا الهجوم.

حيث نلاحظ من هذا أن أي هجوم **attack** يتكون من ثلاث عناصر



(الهدف من الهجوم Motive) + (الطريقة method) + (نقاط الضعف Vulnerability)

العنصر الأول هو **motive** وذلك لان أي هجوم إما ان يكون لهدف أو لدافع معين (**motive , goal or objective**) مثال لهذه الأهداف تعطيل استمرارية العمل (**disrupting business continuity**)، سرقة المعلومات، تنفيذ انتقام من مؤسسه معينه أو سرقة شيء ذات قيمه من مؤسسه ما. هذه الأهداف تختلف من شخص إلى أخر على حسب الحالة العقلية للمهاجم الذي حمله على القيام بهذا العمل. بمجرد امتلاك المهاجم للهدف فانه يستخدم العديد من الطرق والأساليب لاستغلال نقاط الضعف (**exploit vulnerability**) في نظام المعلومات **information system** أو في **security policy** في عملية الهجوم حتى يصل إلى تحقيق هدفه.

SECURITY THREAT التهديدات الأمنية المحتملة.

التهديدات الأمنية المحتملة تنقسم هنا إلى ثلاثة أقسام كالاتى:



- **Natural Threats** التهديدات الطبيعية

التهديدات الطبيعية تشمل الكوارث الطبيعية مثل الزلازل **earthquake** او الفيضانات **floods** او الأعاصير **hurricanes** أو أي كارثه طبيعية أخرى التي لا يمكن إيقافها أو التحكم فيها.
المعلومات التي يتم تدميرها أو فقدانها نتيجة التهديدات الطبيعية لا يمكن منعها حيث لا يمكن توقع وقت حدوثها واقصى ما يمكن فعله هو وضع بعض الخطط الأمنية التي تمكنك من عدم فقد هذه المعلومات مثل خطط الطوارئ واسترجاع البيانات عند الفقدان أو التدمير.

- **Physical Threats** التهديدات الفيزيائية

هذا النوع من التهديد ينتج نتيجة تلف أي جزء من الأجهزة المستخدمة سواء بواسطة الحريق أو الماء أو السرقة أو التداخلات الفيزيائية (**physical impact**) وأيضا مصادر الطاقة التي من الممكن أن تؤدى إلى تلف بعض الأجهزة (**hardware damage**).

- **Human Threat** التهديدات البشرية

هذا النوع من التهديديات ينتج نتيجة الهجمات سواء من داخل المنظمة (**Insider**) أو من الخارج (**Outsider**).

- **Insider Attack (الهجمات من الداخل):** تعتبر الأخطر والتي تتم بواسطة الموظفين من داخل المنظومة او من قبل شخص ساخط. وتعتبر الأخطر لان المهاجم يعرف الكثير مثل الوضع الأمني (**security posture**) الخاص بأنظمة المعلومات.
- **Outsider Attack (الهجمات من الخارج):** تتم بواسطة أشخاص آخرين من الخارج الذين يملكون بعض من الخبرة التي تمكنهم من معرفة الوضع الأمني لنظام المعلومات.

هذا النوع من التهديد ينقسم هو الأخر إلى ثلاث أنواع أخرى كالاتى:





Network Threats .A:

الشبكة Network: هي عبارة عن ربط جهازين حاسوب فأكثر (مجموعة من الأجهزة) مع بعضهما البعض من خلال قنوات اتصال **communication channel** وذلك لتبادل البيانات والموارد **computer resources** مثل (الطابعات، الملفات ... وغيرها). ومع مرور هذه البيانات من خلال قنوات الاتصال **communication channel** فإنه من الممكن دخول شخص ما عنوةً الى هذه القنوات وسرقة ما بها من معلومات.

لذلك فان المهاجم الهاكر يعرض العديد من التهديدات من خلال الشبكة ومن هذه التهديدات كالاتى:

1. Information gathering (جمع المعلومات)
2. sniffing and eavesdropping (التنصت والتجسس)
3. spoofing (التنصت)
4. session hijacking and man-in-middle attack
5. sql injection
6. ARP Poisoning
7. Denial of service attack
8. comprised key attack



Host Threats .B:

هذا النوع من التهديد يتم توجيه إلى النظام الحالي الذي يحمل المعلومات القيمة التي يريدها المهاجم مباشرة (عن طريق الاتصال المباشر). حيث يحاول المهاجم من كسر الوضع الأمني للنظام الذي يحمل هذه المعلومات ومن هذه التهديدات كالاتى:

1. Malware attacks
2. Target Footprinting
3. Password attacks
4. Denial of service attacks
5. Arbitrary code execution
6. Unauthorized access الدخول عنوه أي من غير إن يكون مصرح له بالدخول.
7. Privilege escalation
8. Back door attacks
9. Physical security threats

Application Threats.C

تطوير أي تطبيق أو إنشائه مع عدم الاهتمام بالأوضاع الأمنية الخاصة به. قد يؤدى إلى وجود بعض الثغرات الأمنية في هذا التطبيق وقد ينتج عن هذه الثغرات ثغرات أخرى في تطبيقات أخرى. حيث أن المهاجم يستفيد من هذه الثغرات في تنفيذ هجماته لسرقة المعلومات أو تدميرها ومن هذه التهديديات كالاتى:

1. Data/Input validation
2. Authentication and Authorization attacks
3. Configuration management
4. Information disclosure
5. Session management issues
6. Cryptography attacks
7. Parameter manipulation
8. Improper error handling and exception management
9. Auditing and logging issues

INFORMATION WARFARE (حرب المعلومات)

المصطلح (**Information Warfare/InfoWar**) يشير إلى استخدام تكنولوجيا المعلومات والاتصالات **ICT** في الحصول على بعض المزايا التنافسية من الشركات المنافسة أو بمعنى أخر هو سرقة المعلومات من الشركات المنافسة.

أو بمعنى أخر هو اصطلاح ظهر في بيئة الإنترنت للتعبير عن اعتداءات تعطيل المواقع وإنكار الخدمة والاستيلاء على المعلومات، وكما يشير الاصطلاح فان الهجمات والهجمات المقابلة هي التي تدل على وجود حرب حقيقية، وبما إنها حرب فهي حرب بين جهات تتناقض مصالحها وتتعارض مواقفها، لهذا تكون في الغالب هجمات ذات بعد سياسي، أو هجمات منافسين في قطاع الأعمال. ولذا وصفت حملات الهاكرز اليوغسلافيين على مواقع الناتو أبان ضربات الناتو بانها حرب معلومات ، ووصفت كذلك هجمات المخترقين الأمريكان على مواقع صينية في اطار حملة أمريكية على الصين تحت ذريعة حقوق الأنسان والتي تمت بدعم حكومي أمريكي بانها حرب معلومات ، وأشهر

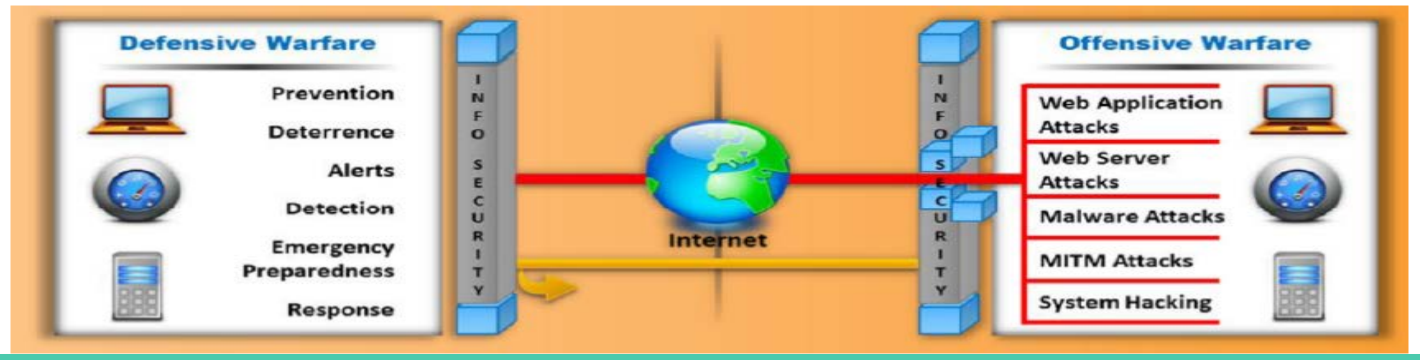
حروب المعلومات القائمة حتى الأن المعركة المستعرة بين الشباب العرب والمسلم وتحديدا شباب المقاومة اللبنانية والمدعومين من خبراء اختراق عرب ومسلمين ، وبين جهات تقنية صهيونية في اطار حرب تستهدف إثبات المقدرات في اختراق المواقع وتعطيلها أو الاستيلاء على بيانات من هذه المواقع . وهذا الاصطلاح في حقيقته اصطلاح إعلامي أكثر منه أكاديمي، ويستخدم مرادفا في غالبية التقارير لاصطلاح الهجمات الإرهابية الإلكترونية ونجده لدى الكثيرين اصطلاح واسع الدلالة لشمول كل أنماط مخاطر وتهديدات واعتداءات وجرائم البيئة الإلكترونية، ونرى قصر استخدامه على الهجمات والهجمات المضادة في ضوء حروب الرأي والمعتقد لتمييزه عن بقية أنشطة تعطيل المواقع التي لا تنطلق من مثل هذه الأغراض.

:Defensive InfoWar

يشير إلى جميع الاستراتيجيات والمبادرات التي تستخدم للدفاع ضد هذا النوع من الهجمات (**ICT assets**).

:Offensive InfoWar

يشير إلى **InfoWar** التي تستخدم للهجوم على المؤسسات (**ICT assets**) في الشركات المنافسة.



IPV6 SECURITY THREATS (التهديدات الأمنية من استخدام IPV6)

IPv6 مقارنة بـ IPv4 فانه يملك تحسينات امنيه افضل منه والتي تصل بك إلى مستوى اعلى من الأمان والخصوصية للمعلومات التي تمر عبر الشبكة ولكن مع ذلك فانه يحمل بعض التهديدات كالاتى:

Auto-Configuration threat-1

IPv6 يدعم الإعداد الألى (**Authconfig**) لعناوين الشبكة (**IP**), والتي تترك المستخدم عرضه للهجوم عبر بعض الثغرات اذا لم يتم الإعداد الصحيح والأمن من البداية.

Unavailability Reputation-based Protection-2

بعض الحلول الأمنية الحالية تعتمد على استخدام **reputation of IP address** (عناوين IPمشهوره أو معروفه) في تصفية بعض المصادر المعروفة لل **malware**. والتي تحتاج إلى وقت حتى يتم تطويرها لكي تشمل عناوين **IPv6**.

Incompatibility of Logging Systems-3

IPv6 يستخدم عناوين ذات حجم 128 bit والتي يتم تخزينها على هيئة 39 حرف ورقم, ولكن **IPv4** يستخدم عناوين ذات أحجام 32 bit وتخزن على هيئة 15 رمز. لذلك فان عمليات التسجيل **logging solutions** في الأنظمة المعتمدة على **IPv4** من الممكن إنها لن تعمل مع الشبكات القائمة على **IPv6**.

Rate Limiting Problem-4

يستخدم مديري الأنظمة **Admin**استراتيجيات الحد (rate limiting strategy) لإبطاء أدوات المهاجم أليا (Automated attack tool) لكن هذا سوف يكون صعبا عند استخدامه مع عناوين ذات أحجام 128 bit.

التهديدات التي تكمن نتيجة استخدام IPV6

Default IPv6 Activation-1

IPv6 من الممكن أن يفعل أليا بدون علم مديري النظام (**ADMIN**), والتي يؤدى إلى عدم فاعلية الأوضاع الأمنية القائمة على **IPv4**.

Complexity of Network Management Tasks-2

مديري النظام (**admin**) دائما ما يختاروا عناوين **IPv6** سهلة الحفظ مثل (::10, ::20, ::FOOD, ::C5C0) وغيرها والتي من السهل توقعها بالنسبة للمهاجم.

Complexity in Vulnerability Assessment-3

IPv6 ذات أحجام 128 bit يجعل فحص بنية الأنظمة (**infrastructure**) من اجل كشف المتسللين والثغرات عمليه معقده.

Overloading of Perimeter Security Controls-4

IPv6 يحمل عنوان ثابت في **header** ذات حجم **40 byte** مع **add-on** (extension header) قد تكون مقيده والتي نحتاجها في بعض العمليات المعقدة بواسطة بعض أدوأة التحكم الأمن (security control) للشبكة مثل routers, security gateways, firewall و IDS.

IPv4 to IPv6 Translation Issues-5

ترجمة الحزم من **IPv4** إلى **IPv6** من الممكن أن يؤدى تدمير الحزم أو ينتج عن سوء تنفيذ هذه الترجمة (poor implementation).

Security Information and Event Management (SIEM) Problems-6

كل عميل يستخدم **IPv6** يحمل عناوين عده من **IPv6** وليس عنوان واحد مما يؤدى إلى التعقيد في ملفات **log** والأحداث **event**.

Denial-of-service (DOS)-7

زيادة التحميل على امن الشبكة وأجهزة التحكم يؤدى إلى تقليل إتاحة موارد الشبكة، والتي تؤدى إلى الهجمات من النوع **DOS**.

Trespassing-8

الميزات المستقبلية لعناوين **IPv6** التي يتم استكشافها من الممكن أن تستغل من قبل المهاجمين في اجتياز الشبكة الخاصة بك من اجل الوصول إلى موارد الشبكة المقيدة (**restricted resources**).

HACK CONCEPT 1.4 (مفهوم الهاكنج)

- **ما هو الفرق بين الهاكر المدمر(Hacking) والهاكر الأخلاقي (Ethical hacking)؟**



التهكير المدمر hacking

يشير إلى استغلال ثغرات الأنظمة(**vulnerability**) والأخلال بالضوابط الأمنية (**compromising security controls**) للحصول على الدخول الغير مصرح به (**unauthorized access**) لموارد النظام. هذا يشمل تعديل النظام (**modifying system**) أو بعض مميزات البرامج (**application feature**) لتحقيق الهدف.



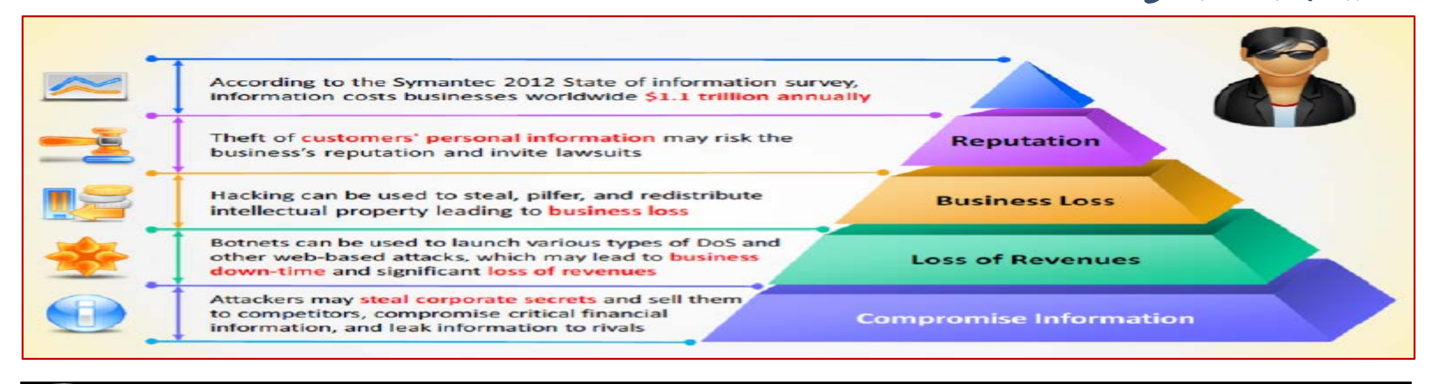
التهكير الأخلاقي Ethical hacking

يشمل استخدام أدوات التهكير وبعض التقنيات والحيل لتعريف الثغرات وذلك للتأكد من امن النظام. وهذا يركز على استخدام تقنيه مشابه للتهكير المدمر لكشف الثغرات في النظام الأمن.

- **ما هو تأثير الهاكر المدمر؟**

1. تلف وسرقة المعلومات.
2. استخدام أجهزة كمبيوتر في التهكير على أخر.
3. استخدام back door
4. سرقة البريد الإلكتروني من اجل الأرقام السرية.
5. سرقة وتدمير الأجهزة.

- **تأثير الهاكر المدمر على الأعمال:**



من هو الهاكرز؟

هو عباره عن شخص محترف يمكنه اختراق الأنظمة والشبكات بطريقه غير قانونيه أو بدون تصريح من أجل تدمير أو سرقة المعلومات الحساسة أو أداء بعض الهجمات الأخرى على الأجهزة الأخرى. وهذا الشخص يتميز بأنه يملك ذكاء مع مهارات جيده في علم الكمبيوتر مع المقدرة على إنشاء وفحص برامج وأجهزة الكمبيوتر.

بعض المهاجمين لدهيم هواية في رؤية كم العدد من الأجهزة والشبكات الذي اختراقها. البعض الأخر يستخدم هذا لكسب المعلومات أو لفعل شيء غير قانوني مثل سرقة معلومات الاستثمارية أو معلومات كارت الائتمان (**ATIM**)أو الرقم السري للبريد الإلكتروني وغيرها.

أنواع الهاكرز:



Black Hats (المخترق ذو القبعة السوداء)

هم أفراد لديهم مهارات استثنائية في علم الحوسبة(**computer science**) ، اللجوء إلى أنشطة ضارة أو مدمرة، كما أنهم معروفين أيضا باسم **كراكرز** (**crackers**).

هؤلاء الأفراد دائم ما يستخدمون مهاراتهم في الأنشطة التدميرية والتي تسبب ضرر كبير للشركات والمؤسسات والأفراد. هؤلاء يستخدمون مهاراتهم في إيجاد الثغرات في الشبكات المختلفة والتي تشمل أيضا المواقع الحكومية ومواقع الدفاع والبنوك وهكذا.

بعضهم يفعل ذلك من اجل أحداث ضرر أو سرقة معلومات أو تدمير بيانات أو كسب المال بطريقه سهل عن طريق قرصنه الرقم التعريق لعملاء البنوك.



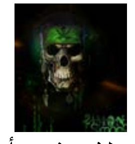
White Hats (المخترق ذو القبعة البيضاء)

هم أفراد يعتنقون مهارات القرصنة (الاختراق) ويستخدمون هذه المهارات من اجل الأهداف الدفاعية؛ كما أنهم معروفين أيضا باسم **المحللين الأمنين** (**security analysts**). في هذه الأيام فان معظم الشركات يملكون محللين امنين من اجل حماية أنظمتهم ضد الهجمات المختلفة. هؤلاء يساعدون الشركات لتامين الشبكات الخاصة بهم.



Gray Hats (المخترق ذو القبعة الرمادية)

هم أفراد لديهم مهارات الهاكر يستخدمونها في الهجوم والدفاع على حد سواء في أوقات مختلفة. وهؤلاء يقعون بين **Black Hats** و**White Hats**. هؤلاء يمكنهم أيضا مساعدة الهاكر في إيجاد الثغرات المختلفة في الأنظمة والشبكات وفى نفس الوقت يقومون بمساعدة المؤسسات في تحسين منتجاتهم (**software and hardware**) عن طريق جعلها أكثر أمانا وهكذا.



Suicide Hackers (الهاكر المنتحرون)

ويطلق علية أيضا الهاكر المنتحر لأنه يشبه إلى حد كبير الشخص الذي يقوم بتفجير نفسه غير مهتم بحياته من اجل هدف ما. وهم عباره عن أفراد يهدفون إلى إسقاط البنية التحتية الحيوية لسبب ما سبب لا يقلقون بشأن 30 عاما في السجن نتيجة أفعالهم ولا يخفون أنفسهم بعد القيام بالهجمة أي بمعنى أخر يسرقون علانيتا. ولقد انتشر هذا النوع في السنوات الأخيرة.



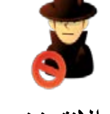
Script Kiddies

هو هاكر ليس لديه مهارات الهاكر ولكن يتحايل على الأنظمة باستخدام بعض الاسكربات والأدوات والتطبيقات التي تم تطويرها بواسطة الهاكرز الحقيقين. وهؤلاء من السهل لهم استخدام التطبيقات والاسكربات في اكتشاف الثغرات في الأنظمة المختلفة. هذا النوع من الهاكر يركز في الأساس على **كمية الهجمات** أكثر من **قوة وفاعلية الهجمة** التي يقوم بإنشائها.



Spy Hackers

هم عباره عن افراد يتم تأجيرهم من قبل المنظمات المختلفة لاختراق والحصول على أسرار من المنظمات المنافسة لهم.



Cyber Terrorists (إرهاب العالم الإلكتروني)

هي هجمات تستهدف نظم الكمبيوتر والمعطيات لأغراض دينية أو سياسية أو فكرية أو عرقية. وتعتبر جرائم إتلاف للنظم والمعطيات أو جرائم تعطيل للمواقع وعمل الأنظمة. وهي ممارسات لذات مفهوم الأفعال الإرهابية لكن في بيئة الكمبيوتر والإنترنت وعبر الإفادة من خبرات الكراكرز وهذا النوع من الهاكر يعتبر الأكثر خطورة لأنه لن يخترق المواقع الإلكترونية فحسب بل من الممكن منطقه بأكملها.



State Sponsored Hackers

هم عباره عن أفراد يتم تأجيرهم بواسطة الحكومات من اجل الاختراق والحصول على معلومات على درجه عالية من السرية وتدمير بعض أنظمة المعلومات الأخرى للحكومات الأخرى.



:HACKTIVISM

هو عمل لتعزيز أجندة سياسية عن طريق القرصنة، خاصة عن طريق تشويه أو تعطيل بعض المواقع. والشخص الذي يقوم بهذه الأشياء يسمى **hacktivist**. أو بمعنى أخر (هذا يشير إلى فكرة القرصنة لأسباب)

هؤلاء الأشخاص يزدهرون في البيئة حيث توجد المعلومات التي يمكن الوصول إليها بسهولة. وهذا يهدف إلى إرسال رسالة من خلال أنشطة القرصنة واكتساب الرؤية من أجل قضية معينه. ومعظم الأهداف إما أن تكون الوكالات الحكومية، والشركات متعددة الجنسيات، أو أي كيان آخر ينظر إليها على أنها كيان سيئ (**bad or wrong**) من وجهة نظر هؤلاء الأشخاص. ولكن يبقى الواقع، أن اكتساب الوصول الغير مصرح به هو جريمة، مهما كان القصد من ذلك.

أو بمعنى أخر هم يقومون بعملية القرصنة لسبب معين قد يكون بدافع الانتقام، أو أسباب سياسية أو اجتماعية أو إيديولوجية، أو للتخريب، والاحتجاج والرغبة في إذلال الضحايا.

HACK PHASE 1.5 (مراحل القرصنة)

هذا يشمل الاتي:

1-Reconnaissance عملية جمع المعلومات (الاستطلاع)
2-Scanning فحص
3-Gaining Access الدخول إلى الهدف
4-Maintaining Access يحافظ على الدخول
5-Clearing Tracks ينظف أي إشارة له

- **Reconnaissance**

يطلق عليها أيضا **preparatory phase** أي المرحلة التحضيرية والتي فيها يقوم المهاجم بجمع أكبر قدر ممكن من المعلومات عن الهدف لتقيمه قبل تنفيذ هجمته. أيضا في هذه المرحلة المهاجم يهتم بالاستخبارات التنافسية لمعرفة المزيد عن الهدف. هذه المرحلة تشمل أيضا **network scanning** (فحص الشبكة) سواء من الداخل أو الخارج بدون دخول على النظام.

هذه المرحلة هي المرحلة التي عن طريقها يضع المهاجم استراتيجيات الهجوم والتي من الممكن أن تأخذ بعض الوقت حتى يحصل على المعلومات المهمة.

جزء من هذه المرحلة يشمل **الهندسة الاجتماعية** (**social engineering**). الهندسة الاجتماعية أو ما يعرف بفن اختراق العقول هي عباره عن مجموعه من التقنيات المستخدمة لجعل الناس يقومون بعمل ما أو يفصحون عن معلومات سريه. وتستخدم في عمليات القرصنة في المرحلة الأولى (مرحلة جمع المعلومات) حيث أن الهدف الأساسي للهندسة الاجتماعية هو طرح أسئلة بسيطة أو تافهة (عن طريق الهاتف أو البريد الإلكتروني مع انتحال شخصية ذي سلطة أو ذات عمل يسمح له بطرح هذه الأسئلة دون إثارة الشبهات).

بعض تقنيات الفحص الأخرى هي **Dumpster diving** (الغوص في سلة المهملات) وهي عباره عن عمليه النظر في سلة مهملات بعض المنظمات من اجل الوصول إلى بعض المعلومات الحساسة المستبعدة.

المهاجم أيضا يمكنه استخدام شبكة المعلومات الأنترنت للحصول على بعض المعلومات مثل معلومات الاتصال والشركاء في العمل والتكنولوجيا المستخدمة وبعض المعلومات الحساسة الأخرى ولكن **dumpster diving** تدعمك بمعلومات أكثر حساسيه مثل اسم المستخدم والرقم السري وأرقام الكريدت كارد والحالة المالية ورقم الائتمان الاجتماعي وغيرها من المعلومات الحساسة.

وينقسم Reconnaissance (الاستطلاع) إلى:

- **Passive Reconnaissance**: التعامل مع الهدف ولكن بطريقه غير مباشره للحصول على معلومات؛ مثل سجلات البحث العامة و نشرات الأخبار و الهندسة الاجتماعية و **dumpster diving** وغيرها
- **Active reconnaissance**: ينطوي على التفاعل المباشر مع الهدف باستخدام أي وسيلة؛ مثل استخدام الأدوات للكشف عن المنافذ المفتوحة مكان تواجد الموجه/الراوتر وهكذا.

- **Scanning**

المسح هو ما يفعله المهاجم قبل تنفيذ الهجوم. ويشير المسح إلى فحص الشبكة للحصول على معلومات محددة على أساس المعلومات التي تم جمعها من خلال عملية الاستطلاع (**Reconnaissance**)، يستخدم القراصنة المسح للحصول على نقطة دخول (الثغرة) للبدء في الهجوم، وتتضمن عملية المسح مسح المنافذ، خرائط الشبكة الضعف الأمني، وما إلى ذلك.
المهاجم دائما ما يستخدم الأدوات الجاهزة مثل **network/host scanner** و**war dialers** لإيجاد النظام واكتشاف الثغرات الذي يحتويها.

- **Gaining Access**

هذه المرحلة تعتبر اهم مرحله ويطلق عليها أيضا **potential damage**. وهذه المرحلة تشير إلى مرحلة الاختراق، المخترق يستغل الضعف في النظام، حيث يمكن أن يحدث ذلك على مستوى شبكة محلية (**LAN**) أو الأنترنت أو على مستوى نظام التشغيل أو على مستوى التطبيقات، ومن الأمثلة على ذلك: **buffer overflows، denial of service، session hijacking، password cracking .**

- **Maintaining Access**

وتشير إلى المرحلة التي يحاول فيها المخترق حفظ ملكية الدخول مجددا إلى النظام، من خلال وصول حصري باستخدام **Backdoors**، **Rootkits**، أو **Trojans**، مما يسمح للمخترق بتحميل ورفع الملفات، والتعامل مع البيانات والتطبيقات على النظام المخترق

- **Clearing Tracks**

تشير إلى الأنشطة التي يقوم بها المخترق لإخفاء دخوله إلى النظام، بسبب الحاجة للبقاء لفترات طويلة، ومواصلة استخدام الموارد، وتشتمل إخفاء بيانات الدخول والتغيير في ملف **Log**.

1.6 TYPE OF ATTACKS (أنواع الهجمات)

هناك العديد من الطرق التي تمكن المهاجم من الدخول إلى النظام. ويجب أن يكون الهاكر قادرا على اكتشاف نقاط الضعف والثغرات في النظام حتى يتمكن من الدخول. ومن هذه الطرق كالاتي:

Types of Attacks

I Operating System Attacks

III Application Level Attacks

II Misconfiguration Attacks

IV Shrink Wrap Code Attacks

1-Operating System attacks: حيث هنا يبحث المهاجم عن ثغرات في نظام التشغيل (**OS vulnerabilities**) ويستخدم هذه الثغرات للدخول إلى نظام الشبكة.

2-Application-level attacks: إن معظم التطبيقات/البرامج تأتي مع وظائف وميزات لا تعد ولا تحصى. ولكن مع ندرة من الوقت لإجراء اختبار كامل قبل خروج المنتج إلى السوق. يؤدى الى ان هذه التطبيقات يكون لديها بعض من نقاط الضعف المختلفة والتي قد تصبح مصدرا للهجوم من قبل الهاكر.

3-Misconfiguration attacks: معظم مديري الأنظمة (**Admin**) لا يملكون المهارات الضرورية من اجل صيانة أو إصلاح بعض المسائل/القضايا، والتي من الممكن أن تؤدى إلى أخطاء في عمليات الإعداد. بعض هذه الأخطاء من الممكن أن تكون مصدرا للمهاجم للدخول إلى الشبك هاو النظام الذي يستهدفه.

4-Shrink wrap code attacks: تطبيقات أنظمة التشغيل تأتى بالعديد من ملفات الاسكريبت المبسطة لكي تسهل العمل على مديري الأنظمة (**Admin**)، ولكن مثل هذه الاسكربات تحتوي أيضا على العديد من الثغرات والتي من الممكن أن تؤدى إلى هذ النوع من الهجوم.

OPERATING SYSTEM ATTACKS-1

أنظمة التشغيل، والتي يتم تحميلها اليوم مع الكثير من المميزات، أصبحت تزداد تعقيدا. ومع الاستفادة من الكثير من هذه المميزات التي توفرها هذه الأنظمة من قبل المستخدمين، تجعل النظام عرضة لمزيد من نقاط الضعف، وبالتالي عرضه للقراصنة. أنظمة التشغيل تعمل على تشغيل العديد من الخدمات مثل واجهات المستخدم الرسومية(**GUI**). وهذه تدعم استخدام المنافذ **ports** وطريقة الوصول إلى شبكة الإنترنت، لذلك فهذه تتطلب الكثير من التغير والتبديل للتحكم في هذا. هنا يبحث المهاجم عن ثغرات في نظام التشغيل (**OS vulnerabilities**) ويستخدم هذه الثغرات للدخول إلى نظام الشبكة. لإيقاف المهاجمين من الدخول إلى شبكة الاتصال الخاصة بك، فإن مسؤولي الشبكة أو النظام لابد لهم من مواكبة الاكتشافات والطرق الجديدة المختلف والمتبعة من قبل المهاجمين ومراقبة الشبكة بشكل مستمر. تطبيق التصحيحات والإصلاحات ليست سهلة في الوقت الحاضر لأنها شبكة معقده.
معظم مستخدمي أنظمة التشغيل يقومون بتثبيت العديد من التطبيقات والتي تقوم بعضها بفتح بعض المنافذ **ports** افتراضيا. والتي تسهل على المهاجمين من اكتشاف العديد من الثغرات. تثبيت الباتشات **patches** وملفت الإصلاح **fix-file** لم يعد سهلا مع تعقيدات الشبكة الموجودة في هذه الأيام. وأيضا معظم الباتشات تعمل على حل المشاكل والثغرات الحالية ولكن لا يمكن اعتبارها الحل الدائم.

بعض من هذه الهجمات تشمل الاتي:

Bugs in the operating system
Exploiting specific network protocol implementation
Breaking file system security
Buffer overflow vulnerabilities
Unpatched operating system
Attacking built-in authentication systems
Cracking passwords and encryption mechanisms

APPLICATION-LEVEL ATTACKS-2

يتم إصدار التطبيقات إلى سوق العمل مع العديد من المميزات والعديد من الأكواد المعقدة. ومع الطلب المتزايد للتطبيقات لما تحمله من وظائف ومميزات، أدى إلى إهمال مطوري التطبيقات الوضع الأمني للتطبيق، والذي أعطى الفرصة لوجود العديد من الثغرات. الهاكر يعمل على اكتشاف هذه الثغرات الموجود في التطبيقات باستخدام العديد من الأدوات والتقنيات.

التطبيقات لما بها من ثغرات تصبح عرض للهجمات من قبل الهاكر نتيجة الأسباب الأتية:

1. لمطوري البرامج الجداول الزمنية الضيقة لتسليم المنتجات في الوقت المحدد (**tight schedules to deliver**) والذي يؤدى إلى ظهور التطبيقات في سوق العمل بدون الاختبارات الكافية عليه.
2. تطبيقات البرامج تأتي مع العديد من الوظائف والمزايا.
3. ليس هناك ما يكفي من الوقت لأداء اختبار كامل قبل الإفراج عن المنتجات (**dearth of time**).
4. الأمن في كثير من الأحيان تكون مرحلة لاحقة، ويتم تسليمها فيما بعد باعتبارها عناصر إضافية(**add-on component**) .

ضعف أو عدم وجود خطأ التدقيق (poor or nonexistent error checking) في التطبيقات امر يؤدى إلى الاتي:

1. Buffer overflow attacks (الهجوم بإغراق ذاكرة التخزين المؤقت)
2. Active content
3. Cross-site scripting
4. Denial-of service and SYN attacks
5. SQL injection attacks
6. Malicious bots

بعض الهجمات الأخرى التي تكون على مستوى التطبيقات كالاتي:

1. Phishing
2. Session hijacking
3. Man-in-the middle attacks
4. Parameter/from tampering
5. Directory traversal attacks

امثله على الهجمات على مستوى التطبيقات:

Session Hijacking-1

```
<configuration>
  <system.web>
    <authentication mode="Forms">
    <forms cookieless="UseUri">
  </system.web>
</configuration>
```

TABLE 1.1: Session Hijacking Vulnerable Code

```
<configuration>
  <system.web>
    <authentication mode="Forms">
    <forms cookieless="UseCookies">
  </system.web>
</configuration>
```

TABLE 1.2: Session Hijacking Secure Code

denial of service-2

```
Statement stmnt = conn.createStatement ();
ResultSet rsltset = stmnt.executeQuery ();
stmnt.close ();
```

TABLE 1.3: Denial-of-Service Vulnerable Code

```
Statement stmnt;
try {stmnt = conn.createStatement ();
stmnt.executeQuery (); }
finally {
If (stmnt! = null) {
try { stmnt.close ();
} catch (SQLException sqlexp) { }
} catch (SQLException sqlexp) { }
```

TABLE 1.4: Denial-of-Service Secure Code

MISCONFIGURATION ATTACKS-3

نقاط الضعف في الإعداد **(misconfiguration)** يؤثر على ملقمات/سيرفرات الويب، ومنصات التطبيق، وقواعد البيانات، والشبكات، أو الإطارات**(framework)** التي قد تؤدي إلى الدخول/ الغير المشروع **illegal access** أو احتمالية امتلاك النظام. إذا تم إعداد النظام بشكل خاطئ، مثل عندما يتم تغيير في تصريحات/أذونات الملف، فيؤدى إلى جعله غير آمن.

SHRINK WRAP CODE ATTACKS-4

عند تثبيت نظام التشغيل أو التطبيقات فانه يأتي مع العديد من الاسكربات والتي تسهل على **Admin** التعامل معها. ولكن المشكلة هنا " ليست ضبط " أو تخصيص هذه الاسكربات التي من الممكن أن تؤدى إلى الرموز الافتراضية أو هجوم **shrink-wrap code**.

```
Private Function CleanUpLine(ByVal sLine As String) As String
    Dim lQuoteCount As Long
    Dim lcount      As Long
    Dim sChar       As String
    Dim sPrevChar   As String

    ' Starts with Rem it is a comment
    sLine = Trim(sLine)
    If Left(sLine, 3) = "Rem" Then
        CleanUpLine = ""
        Exit Function
    End If

    ' Starts with ' it is a comment
    If Left(sLine, 1) = "'" Then
        CleanUpLine = ""
        Exit Function
    End If

    ' Contains ' may end in a comment, so test if it is a comment or in the
    ' body of a string
    If InStr(sLine, "'") > 0 Then
        sPrevChar = " "
        lQuoteCount = 0

        For lcount = 1 To Len(sLine)
            sChar = Mid(sLine, lcount, 1)

            ' If we found " '" then an even number of " characters in front
            ' means it is the start of a comment, and odd number means it is
            ' part of a string
            If sChar = "'" And sPrevChar = " " Then
                If lQuoteCount Mod 2 = 0 Then
                    sLine = Trim(Left(sLine, lcount - 1))
                    Exit For
                End If
            ElseIf sChar = """" Then
                lQuoteCount = lQuoteCount + 1
            End If
            sPrevChar = sChar
        Next lcount
    End If

    CleanUpLine = sLine
End Function
```

إذا كان المتسلل هو أو هي يريد الدخول على النظام الخاص بك فانت لن تستطيع أن تفعل شيء أمام هذا ولكن الشيء الوحيد الذي يمكنك القيام به هو جعل الأمر أكثر صعوبة عليه للحصول على نظامك.

1.7 INFORMATION SECURITY CONTROL (التحكم في امن المعلومات)

- **لماذا الهاكر الأخلاقي ضروري ومهم؟**

هناك نمو سريع في مجال التكنولوجيا، لذلك هناك نمو في المخاطر المرتبطة بالتكنولوجيا، والقرصنة الأخلاقية يساعد على التنبؤ بمختلف نقاط الضعف المحتملة في وقت مبكر وتصحيحها دون تكبد أي نوع من الهجمات القادمة من الخارج.

القرصنة الأخلاقية(ethical hacking) : مثل القرصنة يشمل التفكير الإبداعي، واختبار مواطن الضعف والتدقيق الأمني الذي لا يمكنه التأكد من أن الشبكة آمنة.

استراتيجية الدفاع من العمق (Defense-in-Depth Strategy): لتحقيق ذلك، تحتاج المنظمات لتنفيذ استراتيجية "الدفاع من العمق" عن طريق اختراق شبكاتهم لتقدير مواطن الضعف وعرضهم لهذه.

الهجوم المضاد (Counter the Attacks): الهاكر الأخلاقي هو ضروري لأنه يسمح بمجابهة الهجمات التي يشنها القراصنة الخبيثة بطريقة التوقع (**anticipating methods**) والتي يمكن استخدامها لاقتحام نظام.

- **المخترق الأخلاقي يحاول أن يجاوب على الأسئلة التالية:**
  - **ماذا يمكن أن يرى الدخيل على نظام الهدف؟**

مراحل الاستطلاع والمسح (**reconnaissance and scanning**)

  - **ما الذي يمكن أن يقوم به المتسلل بهذه المعلومات؟**

مراحل الوصول والمحافظة على الوصول (Gaining Access and Maintaining Access)

  - **هل يوجد دخيل على النظام؟**

مراحل الاستطلاع وتغطية الأثر (reconnaissance and covering tracks)

  - **هل جميع أجزاء نظام المعلومات يتم حمياته وتحديثه وتمكين الباتشات باستمرار؟**
  - **هل مقاييس امن المعلومات ممتثله لمعاير الصناعة والقانون؟**

- **لماذا تقوم المؤسسات بتعين المخترقين الأخلاقيين؟**

1. لمنع القراصنة من الدخول إلى قسم المعلومات.
2. لمكافحة الإرهاب ومخالفات الأمن القومي.
3. لبناء نظام يكون قادر على تفادى هجمات القراصنة.
4. لاختبار الوضع الأمني للمؤسسات والمنظمات.

نطاق وحدود القراصنة الأخلاقيين (SCOPE AND LIMITATIONS OF THE ETHICAL HACKERS)

SCOPE

ما يلي نطاق القرصنة الأخلاقية:

- القرصنة الأخلاقية هو عنصر حاسم لتقييم المخاطر، ومراجعة الحسابات، ومكافحة الاحتيال، وأفضل الممارسات، والحكم الجيد.
- يتم استخدامه لتحديد المخاطر وتسليط الضوء على الإجراءات العلاجية، والحد من تكاليف تكنولوجيا المعلومات والاتصالات (**ICT**)عن طريق إيجاد حل لتلك الثغرات.

LIMITATIONS

ما يلي حدود القرصنة الأخلاقية:

- ما لم تعرف الشركات أولا ما الذي يبحثون عنه، ولماذا يتعاقدون مع مورد خارجي لاختراق الأنظمة في المقام الأول؛ وهناك احتمالات بأن لن يكون هناك الكثير لتكسبه من خبرة.
- لذا القراصنة الأخلاقيين الوحيدين الذين يمكنهم أن يساعدوا المنظمات لفهم أفضل لأوضاعهم الأمنية، ولكن الأمر متروك للمنظمة لوضع الضمانات الأمنية على الشبكة.

مهارات الهاكر الأخلاقي ETHICAL HACKER SKILLS:

القرصنة الأخلاقية هي عملية قانونيه يتم تنفيذها بواسطة **pen tester** لإيجاد نقاط الضعف في بيئة تكنولوجيا المعلومات. ولكي يتم هذا يجب أن يتمتع الهاكر الأخلاقي ببعض المهارات كالاتى:

1. خبير في مجال الحوسبة وبارع في مجالات التقنية.
2. يملك معلومات قوية في علم البرمجة والشبكات.
3. معرفته المتعمقة للأشياء المستهدفة، مثل ويندوز ويونكس ولينكس.
4. لدية معرفة مثالية لإقامة الشبكات والأجهزة ذات الصلة والبرمجيات.
5. لدية معرفة مثالية في الأجهزة والتطبيقات التي قدمت عن طريق بائعي الكمبيوتر وأجهزة الشبكات ذات شعبية.
6. ليس من الضروري أن يحمل معرفه إضافية متخصصة في الوضع الأمني.
7. ينبغي أن يكون على دراية ببحوث الضعف.
8. ينبغي أن يكون لديه السيادة في مختلف تقنيات الاختراق أو القرصنة.
9. ينبغي أن يكون على استعداد لاتباع سلوك صارم إذا احتاج الأمر لهذا.

DEFENSE-IN-DEPTH (الدفاع من العمق)

يتم اتخاذ العديد من التدابير المضادة للدفاع من العمق (**Defense-in-Depth**) لحماية أصول المعلومات في الشركة. وتستند هذه الاستراتيجية على مبدأ عسكري أنه من الصعب على العدو هزيمة نظام دفاعي معقد ومتعدد الطبقات من اختراق حاجز واحد. إذا حدث واستطاع الهاكر الوصول إلى النظام، فإن الدفاع من العمق (**Defense-in-Depth**) يقلل التأثير السلبي ويعطي الإداريين والمهندسين الوقت لنشر مضادات جديدة أو محدثة لمنع تكرار هذا الاختراق مرة أخرى.

- الدفاع من العمق (**Defense-in-Depth**) هي استراتيجية الأمن التي توضع عدة طبقات واقية في جميع أنحاء نظام المعلومات.
- يساعد على منع وقوع هجمات مباشرة ضد نظام المعلومات والبيانات بسبب كسر طبقة واحدة لا يؤدي إلا انتقال المهاجم إلى الطبقة التالية.



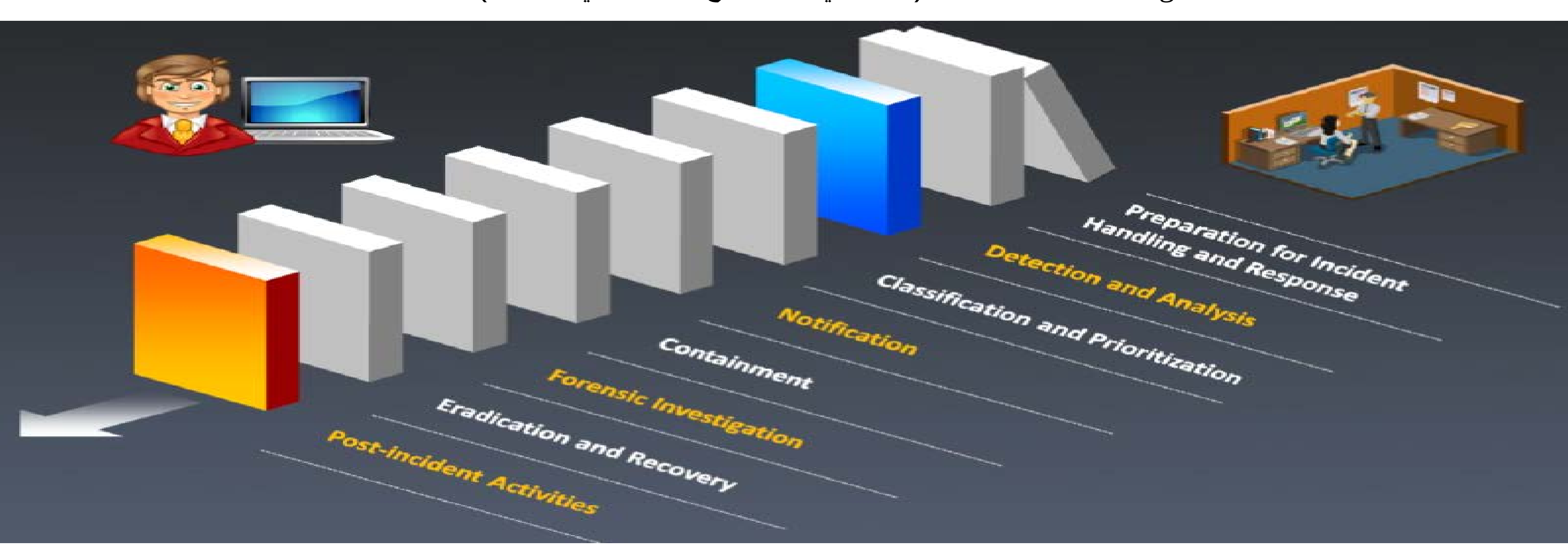
FIGURE 1.4: Defense in Depth Layers Diagram

INCIDENT MANAGEMENT PROCESS (عملية الإدارة الطارئة)

هي مجموعة من العمليات المحددة لتحديد وتحليل، وتحديد الأولويات، وتسوية الحوادث الأمنية لاستعادة النظام إلى عمليات الخدمة العادية في أقرب وقت ممكن ومنع تكرار نفس الحادث.

الغرض من عملية إدارة الحوادث كالاتى:

- improves service quality (تحسين جودة الخدمة)
- Pro-active problem resolution (حل المشاكل الاستباقية)
- Reduces impact of incidents on business/organization (يقلل من تأثير الحوادث على الأعمال التجارية/المنظمات)
- Meets service availability requirements (يلتقي متطلبات الخدمة المتوافرة)
- Increases staff efficiency and productivity (يزيد من كفاءة الموظفين وإنتاجيتهم)
- Improves user/customer satisfaction (يحسن رضا المستخدم / العملاء)
- Assists in handling future incidents (يساعد في التعامل مع الحوادث في المستقبل)



يتم التعامل مع أي حادث وقع في مؤسسة ما وحلها باتباع الخطوات التالية من قبل إدارة الحوادث

سياسات أمن المعلومات INFORMATION SECURITY POLICIES

سياسة الأمن (Security Policy): هو وثيقة أو مجموعة من الوثائق التي تصف الضوابط الأمنية التي ينبغي تنفيذها في الشركة على مستوى عالي لحماية الشبكة التنظيمية من الهجمات سواء من الداخل أو الخارج. تحدد هذه الوثيقة الهيكل الأمني الكامل للمنظمة، وتشمل الوثيقة أهداف واضحة، والأهداف والقواعد والأنظمة والإجراءات الرسمية، وهلم جرا.
هذه السياسات من الواضح إنها تذكر الأصول التي ينبغي حمايتها والشخص الذي يمكنه تسجيل الدخول والوصول إليها، الذين يمكن عرض البيانات المحددة، فضلا عن الناس الذين يسمح لهم بتغيير البيانات، وما إلى ذلك. من دون هذه السياسات، فإنه من المستحيل حماية الشركة من الدعاوى القضائية المحتملة، العائدات المفقودة، وهلم جرا.
على وجه العموم سياسة الأمن هي الخطة التي تُعرّف الاستخدام المقبول أو المرضي لجميع الوسائط الإلكترونية في المنظمة.

سياسات الأمن هي أساس البنية التحتية الأمنية(**Security infrastructure**) . هذه السياسات تعمل على تأمين وحماية موارد المعلومات للمؤسسة وتوفير الحماية القانونية للمنظمة. هذه السياسات مفيدة في المساعدة في تحقيق الوعي للموظفين العاملين في المؤسسة على العمل معا لتأمين اتصالاتهم، وكذلك التقليل من مخاطر ضعف الأمن من خلال عامل الأخطاء البشرية مثل الكشف عن معلومات حساسة إلى مصادر غير مصرح بها أو غير معروفه، الاستخدام الغير لائق للإنترنت، وما إلى ذلك. بالإضافة إلى ذلك، توفر هذه السياسات الحماية ضد الهجمات الإلكترونية والتهديدات الخبيثة، والاستخبارات الأجنبية، وهلم جرا. أنها تتناول أساسا الأمن المادي، وأمن الشبكات، أذون الدخول، الحماية من الفيروسات، والتعافي من الكوارث.

أهداف السياسات الأمنية(SECURITY POLICIES) :

- الحفاظ على الخطوط العريضة لتنظيم وإدارة أمن الشبكات.
- حماية موارد الحوسبة للمنظمة.
- القضاء على المسؤولية القانونية من الموظفين أو أي طرف ثالث.
- ضمان سلامة العملاء ومنع إهدار موارد الحوسبة الخاصة بالشركة.
- منع التعديلات الغير المصرح به على البيانات.
- الحد من المخاطر الناجمة عن الاستخدام الغير مشروع لموارد النظام وفقدان البيانات السرية والحساسة والممتلكات المحتملة.
- التفريق في حقوق الوصول بالنسبة للمستخدم.
- حماية سرية المعلومات الشخصية من السرقة أو سوء الاستخدام، أو الكشف الغير مصرح به.

CLASSIFICATION OF SECURITY POLICY (تصنيف السياسة الأمنية)

إن استراتيجية أمن المعلومات، أو سياسة أمن المعلومات هي مجموعة من القواعد التي يطبقها الأشخاص عند التعامل مع التقنية ومع المعلومات داخل المنشأة وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها.
لإدارة أمنية فعالة، فإن السياسات الأمنية يتم تصنيفها إلى خمسة مجالات مختلفة كالاتي:

- **User Policy (السياسات الأمنية للمستخدم)**
  - هي تتعلق بالموظفين العاملين على النظام التقني. المعني من حيث توفير وسائل التعريف الخاصة بكل منهم وتحقيق التدريب والتأهيل للمتعاملين بوسائل الأمن إلى جانب الوعي بمسائل الأمن ومخاطر الاعتداء على المعلومات. مثال على ذلك: **password management policy**.
- **IT Policy**
  - هذا الجزء مصمم لقسم تكنولوجيا المعلومات للحفاظ على الشبكة آمنة ومستقرة.
  - مثال على ذلك: modification policy، patch updates، server configuration،backup policies
- **General policies**
  - تحديد المسؤولية للأغراض التجارية العامة.
  - مثال على ذلك: crisis management، business continuity plans،high-level program policy
- **Partner policy**
  - السياسة التي يتم تعريفها ضمن مجموعة من الشركاء.
- **Issue-specific policies**
  - يتم تعريف مجالات محددة للقلق ووصف وضع المنظمة من أجل الإدارة على مستوى عالي.



- مثال على ذلك: Physical security policy، personnel security policy

هيكل ومحتوى السياسات الأمنية STRUCTURE AND CONTENTS OF SECURITY POLICIES

هيكل السياسات الأمنية (STRUCTURE OF SECURITY POLICY)

سياسة الأمن هو المستند الذي يوفر الوسيلة لتأمين الأجزاء المادية للشركة، الخاصة بالموظفين والبيانات من التهديدات أو الاختراقات الأمنية. ينبغي تنظيم السياسات الأمنية بعناية فائقة وينبغي إعادة النظر بشكل صحيح للتأكد من أنه لا توجد صيغة يمكن لشخص ما الاستفادة منها. وينبغي أن يشمل الهيكل الأساسي للسياسات الأمنية العناصر التالية:

- وصف تفصيلي لقضايا السياسات الأمنية.
- وصف لحالة السياسة الأمنية
- تطبيق السياسة الأمنية.
- تحديد وظائف المتضررين من السياسة.
- عواقب محددة من شأنها أن تحدث إذا كانت السياسة غير متوافقة مع المعايير التنظيمية.

محتوى السياسات الأمنية (CONTENTS OF SECURITY POLICY)

- **المتطلبات لوضع مستوى عالي من سياسات الأمن high-level security requirements** : هذا يوضح متطلبات النظام لوضع السياسات الأمنية التي سيتم تنفيذها. وهذا يشمل أربعة متطلبات كالاتى:
  - **المتطلبات لانضباط الأمن Discipline security requirements** : هذه المتطلبات تشمل السياسات الأمنية المختلفة مثل أمن الاتصالات، وأمن الحاسوب، وأمن العملية، الانبثاق الأمن، وأمن الشبكات، وأمن الأفراد، وأمن المعلومات والأمن المادي.
  - **المتطلبات للحفاظ على الأمن safeguard security requirement** : هذه المتطلبات تحتوي أساسيا على التحكم في الوصول، الأرشيف، والتدقيق **audit**، المصداقية**authenticity** ، التوافر، السرية، التشفير، التحديد والتوثيق، النزاهة **integrity**، الواجهات، وضع العلامات، عدم الأنكار**non-repudiation** ، إعادة استخدام كائن**object reuse** ، الاسترجاع **recovery**، والحماية من الفيروسات.
  - **المتطلبات لإجراء سياسات الأمن procedural security requirement** : هذه المتطلبات تحتوي أساسيا على سياسات الدخول/الوصول، وقواعد المساءلة، وخطط ووثائق استمرارية العمليات (**continuity-of-operations**)
  - **ضمان الأمن assurance security**: وهذا يشمل عرض شهادات التصديق والاعتماد ووثائق التخطيط المستخدمة في عملية الضمان.
- **الوصف لهذه السياسات Policy Description**: يركز على التخصصات الأمنية، والضمانات والإجراءات واستمرارية العمليات، والوثائق. حيث يصف كل جزئية من هذا الجزء من السياسة كيفية قيام معمارية النظام في فرض الأمن.
- **المفهوم ألأمني للعمليات security concept of operation**: يعرف أساسا الأدوار والمسؤوليات ومهام سياسة الأمن. لأنها تركز على المهمة، والاتصالات، والتشفير، وقواعد المستخدم والصيانة، وإدارة الوقت الضائع، واستخدام البرمجيات المملوكة للقطاع الخاص مقابل برمجيات الدومين العام، وقواعد إدارة البرامج التجريبية، وسياسة الحماية من الفيروسات.
- **تخصيص الأمن لتطبيقه على عناصر المعمارية allocation of security enforcement to architecture elements**: يوفر تخصيص بنية نظام الكمبيوتر إلى كل نظام من البرنامج.

أنواع سياسات الأمن (TYPES OF SECURITY POLICY)

سياسة الأمن هو عباره عن مستند يحتوي على معلومات عن طريقة وتخطط الشركة لحماية أصول المعلومات الخاصة بها من التهديدات المعروفة والغير معروفة. هذه السياسات تساعد على الحفاظ على سرية، وتوافر، وسلامة المعلومات. يوجد أربعة أنواع رئيسية من السياسات الأمنية هي كما يلي:

1) **Promiscuous Policy سياسه خفيفة**: تتميز هذه السياسة بعدم وجود أي قيود على الوصول إلى الإنترنت. يمكن للمستخدم الوصول إلى أي موقع، وتحميل أي تطبيق، والوصول إلى كمبيوتر أو شبكة من موقع بعيد. في حين أن هذا يمكن أن يكون مفيدا في الأعمال التجارية للشركات حيث كان الناس الذين يسافرون أو العمل في المكاتب الفرعية تحتاج إلى الوصول إلى شبكات تنظيمية، العديد من التهديدات مثل البرمجيات الخبيثة(**malware**)، والفيروسات، وطروادة موجودة على شبكة الأنترنت. بسبب

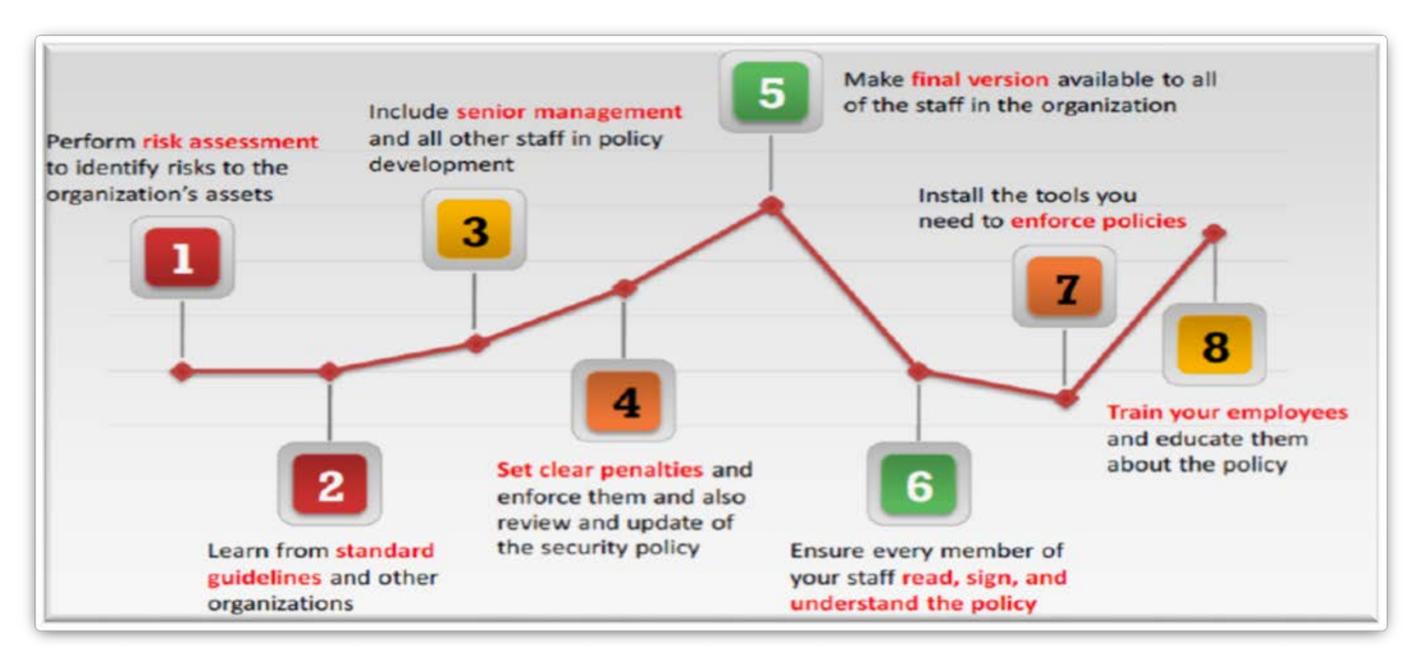
حرية الوصول إلى الإنترنت، وهذه البرمجيات الخبيثة (**malware**) من الممكن أن تأتي كمرفقات دون علم المستخدم. يجب أن يكون مسؤولي الشبكة في حالة تأهب للغاية إذا ما تم اختيار هذا النوع من السياسة.

2) **Permissive Policy سياسه متساهلة**: يتم قبول أغلبية حركة المرور(**internet traffic**) على الإنترنت، ولكن يتم حظر العديد من الخدمات والهجمات الخطيرة المعروفة. ولأنه يعمل على حظر الهجمات المعروفة فقط، فإنه من المستحيل لمسؤولي النظام مواكبة التطور الحالي في الهجمات. الإداريين يحاولون دائما اللحاق بالركب بمعرفة الهجمات والاختراقات الجديدة.

3) **Prudent Policy سياسه حكيمه**: تبدأ هذه السياسة بحظر كافة الخدمات. مسؤولي النظام (**administrator**) يمكنوا فقط الخدمات الأمنة والضرورية بشكل فردي. وهذا يوفر أقصى قدر من الأمان. كل شيء مثل أنشطة النظام والشبكة يتم تسجيله.

4) **Paranoid Policy سياسه مرهبه**: تبدأ هذه السياسة بمنع كل شيء. هناك قيود صارمة على استخدام أجهزة الكمبيوتر الخاصة بالشركة، سواء كان استخدام النظام أو استخدام الشبكة. بسبب هذه القيود على الملقم **server** بشكل مفرط، فإن المستخدمين غالبا ما يحاولون إيجاد السبل حول هذه السياسة.

الخطوات لإنشاء وتطبيق السياسات الأمنية (STEPS TO CREATE AND IMPLEMENT SECURITY POLICIES)



تنفيذ السياسات الأمنية يقلل من خطر التعرض لهجوم. وبالتالي، يجب أن يكون كل شركة السياسات الأمنية الخاصة التي تقوم على أعمالها.
وفيما يلي الخطوات التي يجب أن تتبعها كل مؤسسة من أجل وضع وتنفيذ السياسات الأمنية:

1. تنفيذ لعملية تقييم المخاطر لتحديد المخاطر إلى أصول معلومات المنظمة.
2. التعلم من المبادئ التوجيهية القياسية وغيرها من المنظمات.
3. في وضع السياسات فإنها تشمل الإدارة العليا وجميع الموظفين الآخرين.
4. تعيين عقوبات واضحة وتنفيذها وأيضا مراجعة وتحديث السياسة الأمنية.
5. جعل النسخة النهائية متاحة لجميع الموظفين في المنظمة.
6. ضمان كل فرد من الموظفين أن يقوم بقرائه، وفهم السياسة.
7. تثبيت الأدوات التي تحتاجها لتطبيق سياسة.
8. تدريب موظفيك وتثقيفهم حول السياسة.

أمثله على السياسات الأمنية كالاتى:

وفيما يلي بعض الأمثلة على السياسات الأمنية التي تم إنشاؤها، وتم قبولها، واستخدامها من قبل المنظمات في جميع أنحاء العالم لتأمين أصولها ومواردها الهامة.

- **Acceptable-Use Policy**

يحدد الاستخدام المقبول لموارد النظام.

- **User-Account policy**

يحدد عمليات إنشاء الحساب (**account**). يحدد السلطة، والحقوق، والمسؤوليات الخاصة بحسابات المستخدمين.

- **Remote-Access Policy**

يحدد من له الصلاحية في استخدام الاتصال عن بعد، ويحدد الضوابط الأمنية لهذا الاتصال عن بعد.

- **Information-Protection Policy**

يحدد مستويات حساسية المعلومات، ومن الذي يتاح له الوصول لهذه المعلومات؟ وكيف يتم تخزينها ونقلها؟ وكيف ينبغي حذفها من وسائط التخزين؟

- **Firewall-Management Policy**

يحدد وصول، وإدارة، ورصد الجدران النارية في المنظمات.

- **Special-access Policy**

تحدد هذه السياسة أحكام وشروط منح وصول خاص إلى موارد النظام.

- **Network-Connection Policy**

يحدد الذين يمكنهم تثبيت موارد جديدة على الشبكة، والموافقة على تركيب الأجهزة الجديدة، وتوثيق تغيرات الشبكة، الخ.

- **Email Security Policy**

أنشأت لتحكم الاستخدام السليم للبريد الإلكتروني للشركات.

- **Password Policy**

يوفر مبادئ توجيهية لاستخدام كلمة مرور قوية على موارد المنظمة لحمايتها.

بحوث الثغرات الأمنية (RESEARCH VULNERABILITY SECURITY)

Research Vulnerability هي تقنيات يستخدمها مختبري الاختراق لاكتشاف الثغرات وضعف التصميم التي يمكن من خلالها الهجوم على التطبيقات و أنظمه التشغيل, وتشمل الدراسة الديناميكية للمنتجات والتقنيات و التقييم المستمر لإمكانية الاختراق. هذه البحوث تساعد كل من مسئولي الأمن والمهاجمين. ويمكن تصنيفها على أساس:

- مستوى الخطورة (منخفضة، متوسطة، أو عالية)
- استغلال النطاق (محلي(local)، عن بعد(remotely)).

وتستخدم هذه التقنية:

- لتحديد وتصحيح نقاط ضعف الشبكة.
- لحماية الشبكة من التعرض للهجوم من قبل الدخلاء.
- للحصول على المعلومات التي تساعد على منع المشاكل الأمنية.
- لجمع المعلومات حول الفيروسات.
- للعثور على نقاط الضعف في الشبكة وتنبيه مدير الشبكة قبل حصول الهجوم.
- لمعرفة كيفية التعافي من الهجوم.

أدوات الوصول الى الأبحاث عن الضعف VULNERABILITY RESEARCH WEBSITE

1. **CodeRed Center**

المصدر: http://www.eccouncil.org

هو مصدر امنى شامل لمسؤولي النظام (**admin**) والتي يمكنها أن تعطيك تقرير يومي ودقيق وأحدث المعلومات عن أحدث الفيروسات، وأحصنة طروادة، والبرمجيات الخبيثة، والتهديدات، وأدوات الأمن والمخاطر ونقاط الضعف.

2. **TechNet**

المصدر: http://blogs.technet.com

موقع تم إنشائه من قبل فريق سيرفرات مايكروسوفت (**Microsoft Lync server teams**). يتم قيادتهم من قبل **Lync Server documentation** الكتاب والمعلقين التقنين يأتون من جميع التخصصات والتي تشمل مهندسي الإنتاج ومهندسي الحقول ومهندسي الدعم ومهندسي التوثيق والعديد من التخصصات الأخرى.

3. **Security Magazine**

المصدر: http://www.securitymagazine.com

هذا الموقع يركز على الحلول الفريدة لقادة المؤسسة الأمنية. لقد تم تصميمه وكتابته للمديرين التنفيذيين لرجال الأعمال الذين يقومون بإدارة المخاطر والمؤسسة الأمنية.

4. **SecurityFocus**

المصدر: http://www.securityfocus.com

هذا الموقع يركز على عدد قليل من المجالات الرئيسية التي هي من أعظمها أهميةً للمجتمع الأمني. وعند تصفح الموقع سوف ترى بعض التصنيفات منها كالاتى:

BugTraq يحتوى على قائمه بريديه كبيرة الحجم والإفصاح الكامل لمناقشة تفصيلية والإعلان عن الثغرات الأمنية للكمبيوتر. وهو يعتبر حجر الأساس بالنسبة لمجتمع الأنترنت الأمني.

The SecurityFocus Vulnerability Database يوفر للمتخصصين في مجال الأمن معلومات محدثه عن نقاط الضعف لجميع المنصات والخدمات.

5. **Help Net Security**

المصدر: http://www.net-security.org

هو موقع إخباري يومي عن الأمن والذي يغطي أحدث الأخبار عن أجهزة الكمبيوتر وأمن الشبكات منذ تأسيسها عام 1998. بجانب تغطية للأخبار في جميع أنحاء العالم، فأنه يركز أيضا على جودة المواد الفنية والورقات، ونقاط الضعف، تحذيرات البائعين، والبرمجيات الخبيثة، وتستضيف أكبر مساحة تحميل للبرمجيات الأمنة مع برامج ويندوز، لينكس، ونظام التشغيل **Mac OS X**.

6. **HackerStorm**

المصدر: http://www.hackerstorm.com.uk

هو مورد أمني للقراصنة الأخلاقيين ومختبري الاختراق لوضع خطط اختبار الاختراق أفضل ونطاقات أفضل، وإجراء بحوث عن الضعف.

7. **SC Magazine**

المصدر: http://www.scmagazine.com

هو موقع يتم نشره من قبل **Haymarket Media Inc.** وهو جزء من العلامة التجارية العالمية. ويوجد ثلاثة إصدارات من هذه المجلة.

North America –U.S. and Canada إصدار لأمريكا الشمالية مخصص لأمريكا وكندا

International – U.K and mainland Europe إصدار عالمي مخصص لإنجلترا وبعض البلدان الأوربية.

Asia Pacific online إصدار يتم قراءته بواسطة صانعي القرار لأكثر من 20-دوله موجود في منطقة المحيط الهادي.

المجلة يتم إصدارها شهريا في أول أسبوع في الشهر. وهي أكبر مجله لأمن المعلومات في العالم مع أكبر توزيع في العالم. بدأت العمل سنة 1989.

8. **Computerworld**

المصدر: http://www.computerworld.com

لأكثر من 40 سنه أصبحت computer world المصدر الرئيسي للأخبار التكنولوجيا والمعلومات على مستوى العالم.

9. **HackerJournals**

المصدر: http://www.hackerjournals.com

هو مجتمع أمن المعلومات على الإنترنت. إنها تنتشر الأخبار المتعلقة على وجه التحديد لتهديدات أمن المعلومات والقضايا من جميع أنحاء العالم. وهو عباره عن فريق بحثي يعمل على بحث وتجميع الأخبار من عشرات الآلاف من المواقع لتجلب لك عناوين الأمن الأكثر ملاءمة في مكان واحد. بالإضافة إلى الأخبار، فأنها تستضيف **blogs** والمناقشات، وأشرطة الفيديو التعليمية، ولقد أصبح من أفضل مواقع الإختراق الأكثر شهره في العالم.

10. **WindowsSecurity Blogs**

المصدر: http://blogs.windowsecurity.com

كتب بواسطة المؤلفين المشهورين الذين يقودون خبراء الصناعة.

ما هو اختبار الاختراق (WHAT IS PENETRATION TESTING)؟

اختبار الاختراق (**penetration test**): هو وسيلة لتقييم مستويات الأمن لنظام أو لشبكة معينة. تساعد على حماية الشبكة حيث إذا لم يتم اكتشاف نقاط الضعف في أسرع وقت ممكن فإنك سوف تكون مصدر سهل للهاكر.
خلال اختبار الاختراق، فان الشخص الذي يقوم بهذا الاختبار يحلل كل الإجراءات الأمنية التي تستخدمها المنظمة لتشخيص ضعف التصميم، والعيوب الفنية، ونقاط الضعف. هناك نوعان من الاختبار كالاتى:

- **الصندوق الأسود (black box)**

هو إنشاء هجوم من قبل أشخاص ليس لديهم معرفة مسبقة عن البينة التحتية لفحصها.

- **الصندوق الأبيض (white box)**

هو إنشاء هجوم من قبل أشخاص لديهم معرفة كاملة عن البنية التحتية للشبكة.

بمجرد الانتهاء من الاختبارات فان الشخص المسئول عن الاختبارات (**pen tester**) يبدا في إعداد تقارير والتي تشمل جميع نتائج الاختبار والتي تبين مناطق الضعف التي تم إيجادها.

وتشمل هذه التقارير تفاصيل عن نتائج نشاط الاختراق، ونقاط الضعف مفصلة وإجراءات الوقاية والاقتراحات وعادة ما يكون تسليمها في شكل نسخة مطبوعة لأسباب أمنية.

ما أهمية PEN TESTER؟

- تحديد التهديدات التي تواجه أصول المعلومات في المؤسسة
- تخفيض تكاليف أمن تكنولوجيا المعلومات للمؤسسة وتوفير أفضل عائد من الاستثمار الأمن (**ROSI**) حسب تحديد وحل نقاط الضعف. (**ROSI = Return On Security Investment**)
- توفير المنظومة مع الضمان: من خلال تقييم شامل للمنظومة الأمنية والتي تغطي السياسة(**policy**)، والإجراءات، والتصميم، والتنفيذ.
- الكسب والحفاظ على شهادة لتنظيم الصناعة(**BS7799,HIPAA etc.**) .
- تبني أفضل الممارسات من خلال مطابقة اللوائح القانونية والصناعة.
- الاختبار والتحقق من صحة وكفاءة الحماية الأمنية والضوابط.
- تغيير أو ترقية البنية التحتية القائمة من البرمجيات أو الأجهزة أو تصميم الشبكات.
- التركيز على نقاط الضعف الأكثر شده والتأكيد من الأمن على مستوى التطبيق.
- توفير نهج شامل لخطوات إعداد التي يمكن اتخاذها لمنع الاستغلال.
- تقييم كفاءة أجهزة أمن الشبكات مثل الجدران النارية والموجهات/الراوتر وخوادم ويب.
-

منهج اختبار الاختراق PENETRATION TESTING METHODOLOGY

بمثابة إنك **pen tester**، فيجب عليك ألا تغفل عن أي مورد للمعلومات. يجب أن يتم اختبار جميع مصادر المعلومات الممكنة للبحث عن نقاط الضعف، ليس فقط مصادر المعلومات، ولكن يجب أن يتم اختبار كل آلية وبرنامج تستخدمهم في عملك لأنه إذا كان المهاجم ليس قادراً على خرق نظام المعلومات، فانه أو إنها قد تحاول الوصول إلى النظام ومن ثم إلى المعلومات الحساسة. هناك عدد قليل من الهجمات، مثل هجمات الحرمان من الخدمات (**denial-of-services**)، والتي لا تحتاج إلى الدخول إلى النظام. وبالتالي لضمان أن تحقق فحص لجميع السبل الممكنة لاختراق النظام أو الشبكة، يجب عليك اتباع منهجية اختبار الاختراق. وهذا يضمن النطاق الكامل للاختبار.

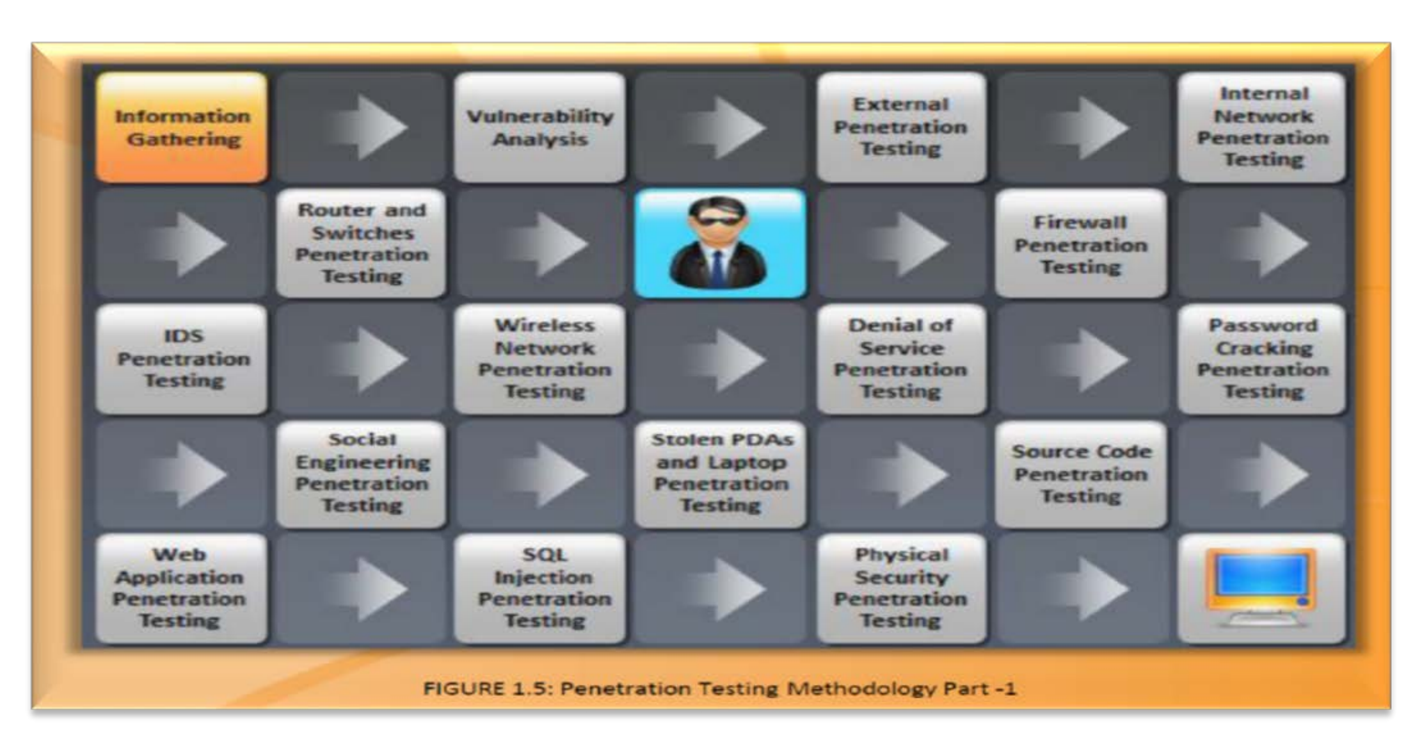


FIGURE 1.5: Penetration Testing Methodology Part -1

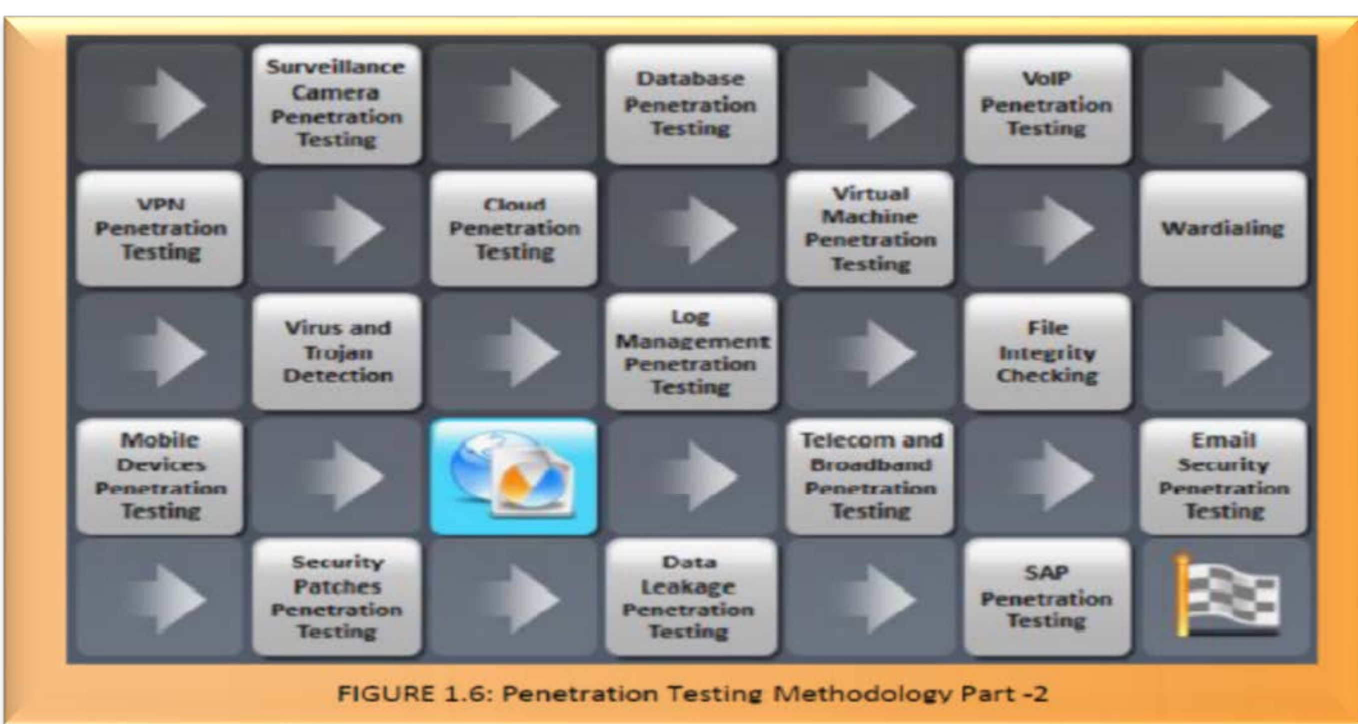


FIGURE 1.6: Penetration Testing Methodology Part -2

لا تنسونا بالدعاء

د. محمد صبحي طيبه